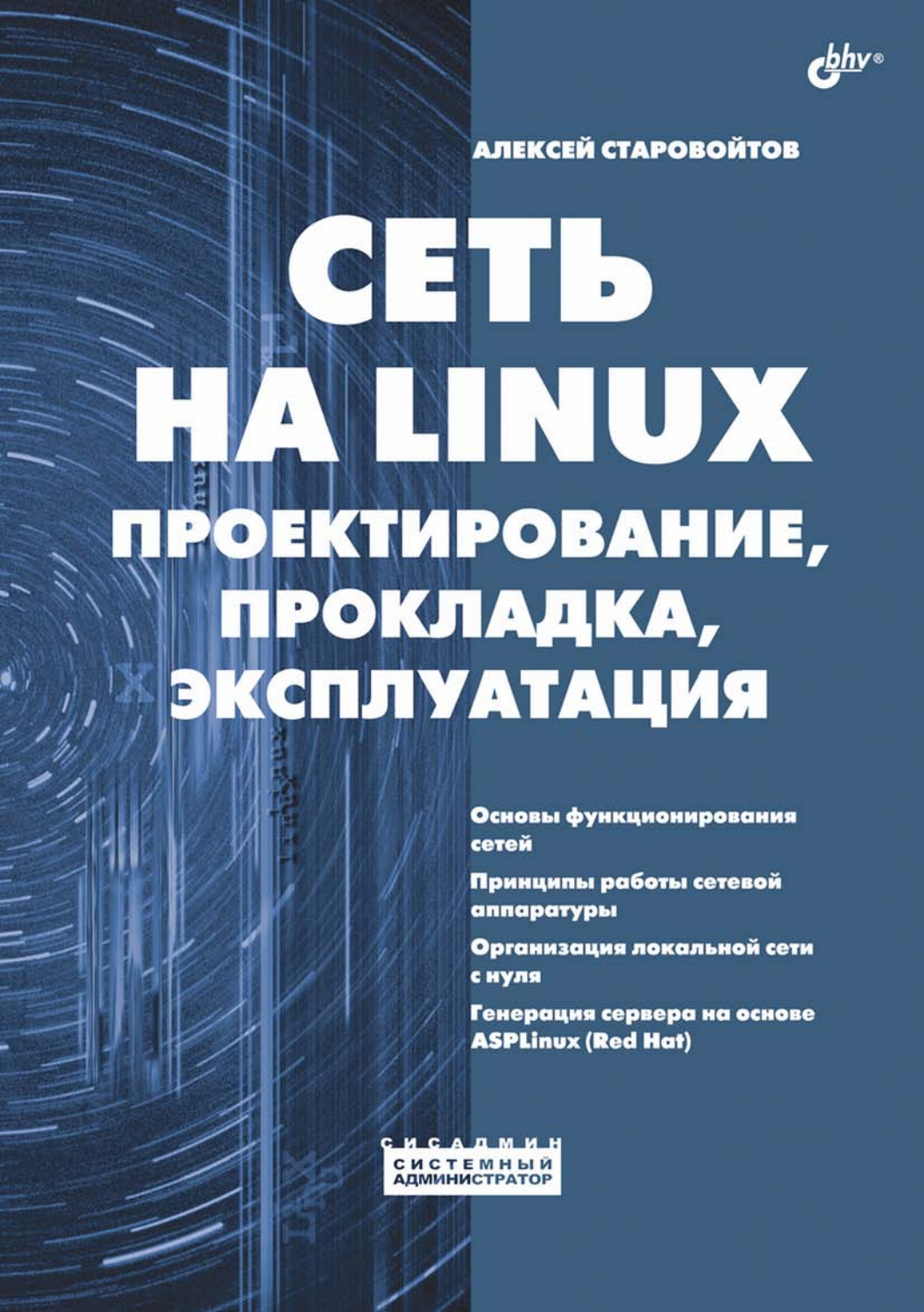

bhv
АЛЕКСЕЙ СТАРОВОЙТОВ
СЕТЬ НА LINUX
ПРОЕКТИРОВАНИЕ, ПРОКЛАДКА, ЭКСПЛУАТАЦИЯ
Основы функционирования сетей
Принципы работы сетевой аппаратуры
Организация локальной сети с нуля
Генерация сервера на основе ASPLinux (Red Hat)
СИСАДМИН
СИСТЕМНЫЙ АДМИНИСТРАТОР

Алексей Старовойтов

СЕТЬ НА LINUX

ПРОЕКТИРОВАНИЕ, ПРОКЛАДКА, ЭКСПЛУАТАЦИЯ

Санкт-Петербург
«БХВ-Петербург»
2006

УДК 681.3.06
ББК 32.973.202
С77

Старовойтов А. А.

С77 Сеть на Linux: проектирование, прокладка, эксплуатация. — СПб.: БХВ-Петербург, 2005. — 288 с.: ил.

ISBN 5-94157-687-0

Рассмотрены практические вопросы по прокладке сети, организации сервера (Apache, Samba, DNS, DHCP) на основе операционной системы Linux и интеграции этого сервера в сетях Windows. Большое внимание уделено повседневной эксплуатации сети. Излагаются основы функционирования сетей и сетевой аппаратуры. Даются практические рекомендации по проектированию и прокладке сетей, проверке и поиску неисправностей. Приводится пример построения локальной сети небольшой фирмы и методика поиска неисправностей без использования специального оборудования. Рассмотрены вопросы антивирусной защиты сервера. Описанная технология может быть использована не только при прокладке и сопровождении сети небольшой фирмы на основе Linux-сервера, но и для организации домашних сетей.

Для системных администраторов и опытных пользователей

УДК 681.3.06
ББК 32.973.202

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Редактор	*Елена Кошлакова*
Компьютерная верстка	*Татьяны Олоновой*
Корректор	*Татьяна Кошелева*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 20.10.05.
Формат $70\times100^{1}/_{16}$. Печать офсетная. Усл. печ. л. 23,22.
Тираж 3000 экз. Заказ №
"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.02.953.Д.006421.11.04 от 11.11.2004 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ОАО "Техническая книга"
190005, Санкт-Петербург, Измайловский пр., 29

ISBN 5-94157-687-0

Оглавление

Введение

Побудительным мотивом к написанию этой книги послужил повышенный интерес к операционной системе Linux и компьютерным сетям, построенным под управлением этой операционной системы. В книге собран опыт автора по прокладке сетей и организации серверов на базе Linux. Уникальность подхода состоит в изложении в одной книге двух связанных между собой вопросов:

1. Прокладка сети и ее эксплуатация.
2. Установка, сопровождение и администрирование Linux-сервера.

Большое количество графического материала иллюстрирует повествование, а листинги конфигурационных файлов делают изложение более понятным.

О чем эта книга

Книга рассматривает практические аспекты в области проектирования и прокладки локальных сетей, а также модернизации существующей сети. Кроме того, предметом книги является создание сервера небольшой организации на основе Linux.

Помимо описания необходимых теоретических основ построения сетей и установки сервера, приводятся рекомендации и примеры, позволяющие быстро перейти от теории к практике. Применение Linux изложено для ASPLinux 7.3 Server, однако подходит для любого из существующих дистрибутивов, в частности, для Red Hat и его клонов. В книге также рассмотрены вопросы повседневной эксплуатации сети и ремонта.

Для кого эта книга

Книга может быть полезна как пользователям, не имеющим опыта работы с Linux и прокладки сетей, так и желающим расширить свои знания, а также системным администраторам начального уровня.

Какова структура книги

Книга построена по принципу от простого — к сложному. Начиная с теоретических основ функционирования протоколов и сетей, читатель постепенно осваивает более сложные вопросы, такие как администрирование и настройка сетевых служб. Книга состоит из трех частей.

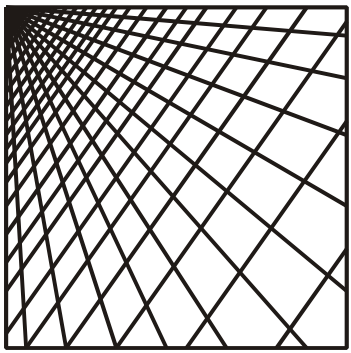
Первая часть описывает функционирование протокола TCP/IP, теоретические принципы построения локальных сетей. Приведены основные определения в области сетевых технологий, основные стандарты построения сетей и их различия.

Вторая часть посвящена прокладке кабельной системы, ее модернизации и тестированию. Рассматривается аппаратура локальных сетей и принципы ее работы. На практическом примере рассмотрено проектирование кабельной системы с использованием витой пары. Рассмотрены инструменты и практические приемы прокладки сети. В заключение второй части даются рекомендации по выбору конфигурации сервера, его сборке. Даны рекомендации по тестированию и поиску неисправности без использования специального оборудования.

Третья часть касается операционной системы Linux. Подробно рассмотрены вопросы инсталляции операционной системы ASPLinux 7.1 Server Edition в контексте решаемых задач, выбор пакетов и настройка графического режима. Основное внимание уделено наиболее частым вопросам начинающих администраторов. Рассмотрены также настройки Linux для интеграции в Windows-сети с использованием программного обеспечения Samba, серверы DNS и DHCP, запуск Apache и Webmin. Отдельное внимание уделено антивирусной защите при помощи программного обеспечения Dr.Web.

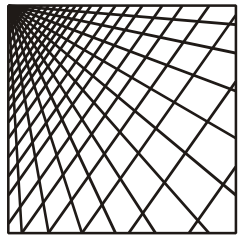
Как связаться с автором

Официальный сайт автора книги **http://www.Linux-75.narod.ru**. Здесь вы можете получить доступ к новым наработкам по тематике, рассмотренной в книге. При желании можно принять участие в работе сайта.



ЧАСТЬ I

Краткие основы функционирования сетей



Глава 1

Характеристика протокола TCP/IP

1.1. Модель OSI

На основании опыта, полученного при создании сетей, в середине 1980 гг. прошлого века была разработана модель, которая сыграла важную роль в развитии сетевых технологий. Речь идет о модели OSI (Open System Interconnection — взаимодействие открытых систем). Модель OSI определяет стандартные уровни взаимодействия систем и функции каждого из уровней. Иными словами, модель OSI является многоуровневым набором протоколов. При развитии программных или аппаратных средств переписывается не весь протокол заново, а лишь необходимая часть.

Модели OSI разделяет средства взаимодействия на семь уровней: прикладной (его еще называют уровнем приложений, строго говоря, не совсем корректно), представления, сеансовый, транспортный, сетевой, канальный и физический (рис. 1.1).

Каждый уровень выполняет определенные функции и обеспечивает связь со смежным уровнем (представляет вышестоящему уровню определенный сервис и может запросить у нижестоящего уровня сервис для себя). Это позволяет обеспечить независимость высоких уровней от технических деталей более низких.

- Прикладной уровень позволяет пользователям или приложениям получать доступ к сетевым ресурсам: файлам, web-страницам, принтерам, электронной почте.
- Уровень представления обеспечивает интерпретацию данных и их подготовку для прикладного уровня (на принимающем компьютере), а также прием данных от прикладного уровня в формат сеансового уровня (на передающем компьютере). Этот уровень имеет дело с представлением данных, не меняя их сути. Этот уровень также осуществляет защиту данных в сети (шифрование, например SSL) и сжатие данных.

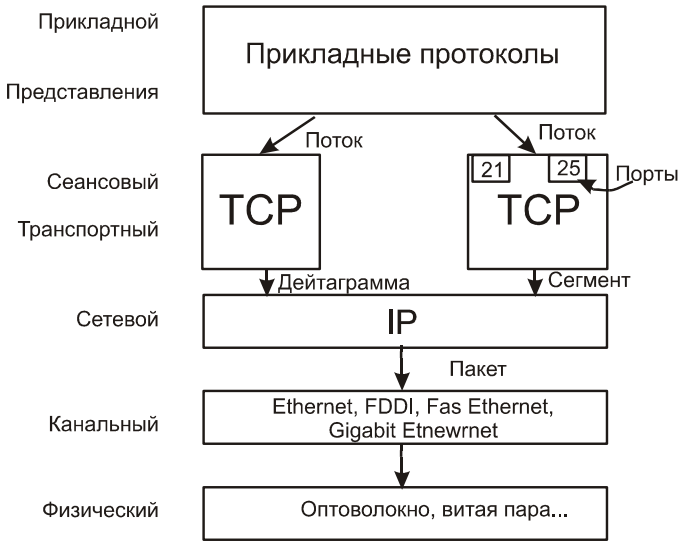


Рис. 1.1. Стек TCP/IP и модель OSI

- Сеансовый уровень устанавливает соединение между двумя компьютерами. Управляет этим соединением, восстанавливает и завершает его при необходимости. Этот уровень также отвечает за синхронизацию и содержит дополнительные функции управления.
- Транспортный уровень обеспечивает вышестоящим уровням передачу данных с необходимой степенью надежности. Он отвечает за распознавание и коррекцию ошибок. Также он определяет класс сервиса: срочность, надежность, возможность восстановления. Самый низкий класс сервиса 0, самый высокий 4.
- Сетевой уровень. Функции сетевого уровня достаточно разнообразны, фактически он образует единую систему, объединяющую сети с различными принципами передачи сообщений.

Прикладной, уровень представления, сеансовый, транспортный и сетевой уровни реализуются программно.

- Канальный уровень реализует связь между сетевым и физическим уровнем, выполняет функции проверки доступности среды, проверяет корректность передачи кадров. Функции канального уровня реализуются сетевыми адаптерами и их драйверами.
- Физический уровень определяет электрические, оптические, механические и другие параметры взаимодействия в сети. Он регламентирует тип физический среды передачи, метод кодирования, скорость передачи. Физический уровень реализуется сетевым адаптером и средой передачи (витая пара, оптоволокно).

1.2. Стек TCP/IP

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol — Протокол управления передачей/Межсетевой протокол) был разработан более двадцати лет назад по инициативе Министерства обороны США и внедрен в сети ARPANET и MILNET. Из объединения этих сетей и родился Интернет. Большую роль в популяризации TCP/IP сыграла его реализация в ОС UNIX. Сегодня протокол TCP/IP реализован во всех распространенных операционных системах: MS Windows, Novell, Linux.

Соответствие стека протоколов TCP/IP и модели OSI приведено на рис. 1.1. Набор протоколов TCP/IP захватывает транспортный сетевой и сеансовый уровни. Поверх TCP/IP работают протоколы более высокого уровня: Telnet, SNMP, FTP, HTTP.

Протокол TCP примерно соответствует сеансовому и транспортному уровням модели OSI, с его помощью реализуется сеанс связи между двумя компьютерами. Протокол TCP формирует из потока данных сегменты и контролирует прохождение сегмента по сети. К его функциям относится исправление ошибок и отслеживание прохождения пакетов по сети. При необходимости протокол организует повторную передачу потерянных или поврежденных сегментов. Таким способом достигается необходимая надежность, поскольку протокол IP не отвечает за доставку сообщений. При прохождении данных протокол TCP добавляет к ним свою служебную информацию.

Протокол IP (Межсетевой протокол) отвечает за маршрутизацию сегментов TCP. В его функции входит формирование IP-пакетов из данных на его входе, а также межсетевая адресация. По сути, протокол TCP использует IP-протокол в качестве транспортного средства. При прохождении IP пакета между сетями он упаковывается в соответствующие каждой конкретной сети средства транспортировки. Очень важно, что протокол IP рассматривает каждый IP-пакет как независимую единицу. Здесь нет средств контроля доставки пакетов. Если узел передал IP-пакет, то судьба этого пакета его уже не интересует. Все вопросы обеспечения надежности обеспечивает протокол TCP. Именно он организует повторную передачу, если какой-то из IP-пакетов потерялся. Протокол IP, как и протокол TCP, добавляет к данным служебную информацию своего уровня. Затем пакет продвигается по канальному и физическому уровню, где к нему добавляется соответствующая служебная информация.

Полезно будет вспомнить терминологию, применяемую в этой области.

Поток — данные, поступающие на вход протоколов TCP (и UDP). *Сегмент* — единица данных протокола TCP. *Дейтограмма* — единица протокола UDP. Единица данных протокола IP называется *пакетом*. *Порт* — уникальный идентификационный номер, который протокол TCP присваивает

приложению, использующему его в качестве транспорта. Все порты с номером меньше 1024 используют определенные приложения. Номера портов больше1024 могут использоваться пользователем произвольно. В табл. 1.1 приведены номера портов некоторых известных служб. Номер порта и IP-адрес образуют *гнездо* (socket).

Таблица 1.1. *Номера некоторых стандартных портов*

Номер	Служба	Примечание
20	FTP-DATA	Протокол передачи данных FTP, данные
21	FTP	Протокол передачи данных FTP, управление
23	TELNET	Telnet
25	SMTP	Простой протокол передачи сообщений (Передача почты)
53	DNS	Службы доменных имен
69	TFTP	Упрощенный протокол передачи данных
70	GOPHER	Gopher
80	HTTP	Протокол передачи гипертекста
110	POP3	Post Office Protocol (Получение почты)
156	SQL	Служба SQL

Чтобы различать узлы, входящие в сеть, существует специальная система адресов. Адреса бывают трех типов:

Локальный адрес — адрес, определяемый технологией данной сети. Если речь идет о локальной сети, то это MAC-адрес (адрес, присвоенный производителем сетевой карте или порту маршрутизатора). Этот адрес уникальный, он назначается сетевой карте производителем. Адрес содержит 6 байтов: 3 байта выделяется централизованно под номер производителя, 3 байта назначается самим производителем под уникальный номер изделия. Локальный адрес имеет следующий вид: A7-B8-C4-11-D5-1F.

IP — это адрес, на основании которого протокол IP осуществляет доставку пакетов. Это адрес представляет собой 4 байта. Поскольку оперировать с двоичными цифрами человеку сложнее, то записывается IP-адрес в десятичной системе с разделением байтов точками. Например, адрес компьютера в локальной сети может выглядеть так: 192.168.10.12, на самом деле это 11000000 10101000 00001010 00001100.

Символьное или доменное имя. Поскольку человеку достаточно сложно запоминать комбинации из четырех групп цифр, то в соответствие IP-адресам

были поставлены символьные имена. С таким типом адресов вы сталкиваетесь в Интернете. Подробнее об этом мы поговорим, когда речь пойдет о службе DNS.

Теперь поговорим об IP-адресах подробнее. Собственно IP-адрес состоит из двух частей: номера сети и номера узла в этой сети. IP назначается во время установки или настройки оборудования администратором сети. Для назначения IP-адресов существуют определенные правила. В сети Интернет выдачей IP-адресов заведуют специальные службы (NIC), и выбирать произвольный адрес нельзя. В локальных сетях все немного проще, в принципе вы можете присваивать любые адреса. Однако если локальная сеть подключена к Интернету (или в обозримом будущем подключение произойдет), то при назначении адресов узлов в локальной сети необходимо придерживаться определенных правил. Для того чтобы их лучше понять, рассмотрим классы IP-адресов.

Как вы знаете, одна часть IP-адреса — это номер сети, а другая — номер узла. То, какая часть относится к номеру сети, а какая к номеру узла, определяется по первым битам в IP-адресе. Существуют 5 классов IP сетей (рис. 1.2).

Рис. 1.2. Структура IP-адреса и классы IP сетей

Особыми являются класс D и класс E. Класс D начинается с последовательности 1110 и является групповым адресом — *multicast*. Сообщение, которое содержит адрес класса D, получат все узлы с этим адресом. Класс E начинается с последовательности 11110 и зарезервирован для будущего.

Помимо этих классов, существуют еще так называемые специальные IP-адреса:

- Адрес, состоящий из двоичных нулей, означает адрес узла сгенерировавшего пакет.
- Если в номере сети стоят нули, то считается, что узел назначения принадлежит к той же сети, что и узел, отправивший пакет.
- Пакет, состоящий из одних единиц, рассылается всем узлам в той сети, где находится источник сообщения.

- Если в поле номера узла стоят единицы, такой пакет рассылается всем узлам с указанным номером сети.
- Адрес, начинающийся с 127, предназначен для организации тестирования программ и взаимодействия процессов в рамках одной машины без передачи пакетов в сеть. Этот адрес имеет имя loopback (петля).

Помимо этих ограничений, для назначения IP-адресов в локальной сети существуют еще несколько правил. Для локальных сетей зарезервированы специальные диапазоны адресов:

- в классе A это диапазон 10.0.0.0 – 10.255.255.255;
- в классе B это диапазон 172.16.0.0 – 172.31.0.0;
- в классе C это диапазон 192.168.0.0 – 192.168.225.0.

Для разделения номера узла и номера сети может использоваться маска. Маска — это двоичное число, оно содержит единицы в тех разрядах, которые относятся к адресу сети. Для системы адресации, основанной на классах, маски такие: A — 255.0.0.0, B — 255.255.0.0, C — 255.255.255.0. Используя маски, можно добиться более гибкой системы адресации.

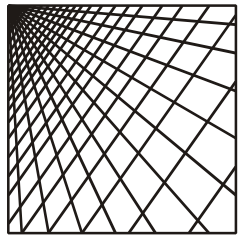
Теперь обратим внимание на то, что у нас есть два объекта: IP-адрес и MAC-адрес (локальный адрес). Эти два адреса не связаны между собой. Для того чтобы IP-пакет попал на нужный локальный узел, необходимо этот пакет перед отправкой в сеть снабдить MAC-адресом, соответствующим IP-адресу назначения. При отсутствии этого адреса у отправителя на помощь приходит ARP-протокол (Address Resolution Protocol — протокол разрешения адреса).

Узел формирует широковещательный ARP-запрос, и все узлы получают его. Затем они сравнивают IP-адрес со своим адресом, при совпадении формируется ответ, в который вкладывается искомый MAC-адрес.

Существует протокол, выполняющий обратную функцию: RARP (Reverse Address Resolution Protocol — протокол обратного разрешения адреса).

С начала 1990-гг. прошлого века началось бурное развитие Интернета, что в конечном итоге привело к дефициту IP-адресов. Одним из выходов из создавшегося положения является внедрение протокола IPv6, в котором для адресации используется уже не $8 \times 4 = 32$ бита, а 128 битов. Также увеличено и число уровней иерархии. Введена двухуровневая иерархия провайдеров и трехуровневая — для абонентов. Это резко повышает количество допустимых адресов и должно снять проблему нехватки свободных адресов.

Совместимость с текущей IPv4-версией обеспечивается ведением специального типа адресов — IPv4 compatible, где в старших 96 разрядах содержаться нули, а младшие 32 соответствуют адресу IPv4. Кроме этого, в протоколе IPv6 реализуются новые технологии защиты.



Глава 2

Технологии локальных сетей

2.1. Кабели, используемые в локальных сетях

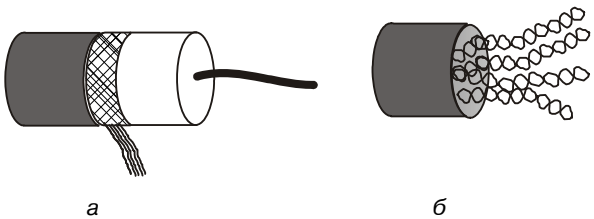
В локальных сетях небольших предприятий на сегодняшний день наиболее используемым стал кабель на основе неэкранированной витой пары UTP. Однако это далеко не единственный кабель, применяемый в современных сетях. Более того, построение сетей исторически началось на других типах кабеля. В некоторых сетях, оставшихся как наследие прошлого, используются коаксиальные кабели. Любой кабель имеет множество характеристик, определяющих возможности его использования. Наиболее важными характеристиками являются:

- активное сопротивление — сопротивление кабеля по постоянному току. Как правило, нормируется на определенную длину, поскольку с увеличением длины кабеля сопротивление растет;
- погонная емкость — это емкость между двумя проводниками или между проводником и оплеткой кабеля. Нормируется тоже на единицу длины кабеля. Погонная емкость приводит к тому, что высокочастотный сигнал затухает по мере продвижения его по кабелю. Погонная емкость является паразитным параметром, и ее стремятся снизить;
- волновое сопротивление (импеданс) представляет собой полное сопротивление кабеля. Как правило, значение сопротивления приводится для определенной частоты, поскольку с ростом частоты оно изменяется;
- затухание — параметр говорит сам за себя. Затухание измеряется в децибелах на единицу длины и частоту сигнала;
- перекрестные наводки. Суть явления в следующем. Если есть два параллельных проводника, и по одному из них идет высокочастотный сигнал, на втором кабеле образуется паразитное напряжение от первого. Величина перекрестных наводок измеряется в децибелах и нормируется на определенную частоту.

Рассмотрим основные типы кабелей, используемых в локальных сетях, и их характеристики.

Коаксиальный кабель

Коаксиальный кабель используется в самых различных областях техники. Кабель представляет собой центральную медную жилу, которая окружена диэлектриком. Затем идет медная оплетка, которая защищает центральную жилу от внешнего излучения, а также предотвращает излучение во внешнюю среду. Наиболее известный среди обывателей коаксиальный кабель — это телевизионный кабель (волновое сопротивление 75 Ом). В компьютерных сетях применяются кабели RG-8 и RG-11 (так называемый "толстый" коаксиальный кабель), их волновое сопротивление 50 Ом, внешний диаметр 0,5 дюйма. Также используются кабели RG-58 ("тонкий" коаксиальный кабель) — волновое сопротивление 50 Ом, внешний диаметр 0,25 дюйма (рис. 2.1, *а*).



а *б*

Рис. 2.1. Коаксиальный кабель и витая пара

Кабель на основе неэкранированной витой пары

UTP (Unshielded Twisted Pair) — неэкранированная витая пара (рис. 2.1, *б*). Представляет собой набор из 4-х пар кабеля, скрученных попарно. Затем эти пары скручены между собой. Витая пара делится на семь категорий (UTP1 − UTP7). Кабели первой и второй категорий сегодня применяются только для телефонных сетей. Кабели третьей, четвертой и пятой категорий широко используются для построений компьютерных сетей. Кабель третьей категории был стандартизирован в 1991 г. для работы на частотах до 16 МГц. Небольшим улучшением кабеля третьей категории послужил кабель четвертой категории, который допускал работу уже на частотах до 20 МГц. Кабель пятой категории разрабатывался специально для работы сетевых высокочастотных протоколов в диапазоне до 100 МГц. Электрические характеристики кабелей UTP3−UTP5 приведены в табл. 2.1.

Таблица 2.1. *Характеристики кабеля UTP3, UTP4, UTP5*

Параметр	UTP3	UTP4	UTP5
Число пар	4	4	4
Волновое сопротивление	100 ± 15 Ом	100 ± 15 Ом	100 ± 15 Ом

Таблица 2.1 *(окончание)*

Параметр	UTP3	UTP4	UTP5
Затухание (dB на 100 м)	4 МГц: 5.6 10 МГц: 9.8 16 МГц: 13.1	4 МГц: 4.3 10 МГц: 7.2 16 МГц: 8.9	16 МГц: 8.2 31 МГц: 11.7 100 МГц: 22
Перекрестное затухание не менее (dB)	4 МГц: 32 10 МГц: 26 16 МГц: 23	4 МГц: 47 10 МГц: 41 16 МГц: 38	16 МГц: 44 31 МГц: 39 100 МГц: 32

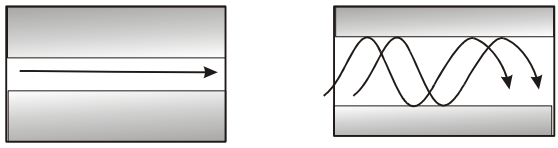
Кабели шестой и седьмой категорий работают на частотах до 200 и 600 МГц, соответственно. Их применение сдерживает относительно высокая цена.

Кабель на основе экранированной витой пары

Shielded Twisted Pair (STP) — экранированная витая пара (рис. 2.2). Особенностью кабеля является наличие у него экрана. Это защищает его от внешних электромагнитных воздействий, а также снижает уровень излучения во внешнюю среду. Кабели на основе STP бывают девяти типов.

В локальных сетях применяется Type 1. Он представляет собой 2 пары скрученных проводов, экранированных оплеткой. По параметрам кабель Type 1 примерно соответствует кабелю UTP пятой категории. Однако его волновое сопротивление 150 Ом. Поэтому при применении его в качестве физической среды в локальных сетях необходимо обращать внимание на то, чтобы сетевое оборудование могло работать с волновым сопротивлением 150 Ом. В противном случае из-за несовпадения волнового сопротивления кабеля и активных сетевых устройств в местах их соединений будут образовываться отраженные волны. Результатом может стать непредсказуемое поведение сети и возникновение сбоев в ее работе.

Недостатком является необходимость хорошего заземления, а также более сложная по сравнению с UTP прокладка кабеля.



а *б*

Рис. 2.2. *а* — одномодовый и *б* — многомодовый оптический кабель

Волоконно-оптический кабель

Волоконно-оптические кабели представляют собой кабель из материала, проводящего свет. (В качестве источников излучения используются либо светодиоды, либо лазеры.) Показатели оптического преломления различны у центральной части и у внешней оболочки. В результате луч света не выходит за пределы центральной части оптического волокна. Различают многомодовые (Multi Mode Fiber — MMF) и одномодовые (Single Mode Fiber — SMF) оптические кабели (рис. 2.2). В многомодовых кабелях используется диаметр внутреннего проводника около 50 мкм. В результате внутри кабеля существует несколько световых лучей. В одномодовых кабелях диаметр внутренней части составляет менее 10 мкм. Это сравнимо с длиной волны используемого светового излучения. В результате световой пучок распространяется вдоль оптического кабеля. Одномодовые кабели имеют более широкую полосу пропускания за счет отсутствия потерь при отражении, однако так как волокно очень тонкое, монтаж одномодового волокна — чрезвычайно трудоемкая процедура, и ей должны заниматься специалисты.

Несмотря на множество преимуществ, у оптического кабеля есть один важный недостаток — более сложный монтаж сети.

2.2. Стандарты сетей

Изначально при разработке технологии локальных сетей разработчики основное внимание уделяли созданию простых, надежных и дешевых способов соединения компьютеров в локальную сеть. Поэтому одним из первых было решение об использовании единой разделяемой во времени среды передачи. С физической точки зрения сеть, объединяющая несколько компьютеров, может иметь различную топологию. Наиболее интересны с точки зрения локальных сетей следующие варианты:

- Общая шина — компьютеры подключены к общему кабелю. Применение такой технологии удешевляет прокладку сети. Однако есть серьезный недостаток — низкая надежность. Любой дефект кабеля или разъема приводит к остановке всей сети.
- Звезда — в этом случае каждый компьютер подключается отдельным отрезком кабеля к устройству, находящемуся в центре сети. Это устройство называется концентратор. Фактически концентратор передает сигнал с одного из своих входов на все выходы, за исключением того, с которого пришел этот сигнал. Основное преимущество (по сравнению с общей шиной) — это более высокая надежность, ведь повреждение отдельного кабеля сказывается только на работе одного участка сети и не затрагивает все остальные.

- Кольцо — данные передаются по кольцу в одном направлении. Незначительным недостатком является то, что при применении кольцевой топологии приходится принимать меры по повышению надежности сети, чтобы выход из строя одного узла не повлиял на работу остальных узлов сети.

Схемы физической топологии приведены на рис. 2.3. Построение сети по принципу общей шины или кольца имеет более низкую надежность и более низкую пропускную способность. Это привело к тому, что в современных локальных сетях небольшого размера, как правило, применяется звездообразная топология. Кроме того, появление новых устройств: мостов, коммутаторов, маршрутизаторов — сняло проблему единой разделяемой среды данных.

Быстрые темпы развития сетевых технологий требовали необходимости принятия стандартов. В начале 1980-х гг. прошлого века был разработан и принят стандарт IEEE 802.x. Основой для его создания послужили существовавшие на тот момент внутрифирменные стандарты ведущих производителей компьютерной техники.

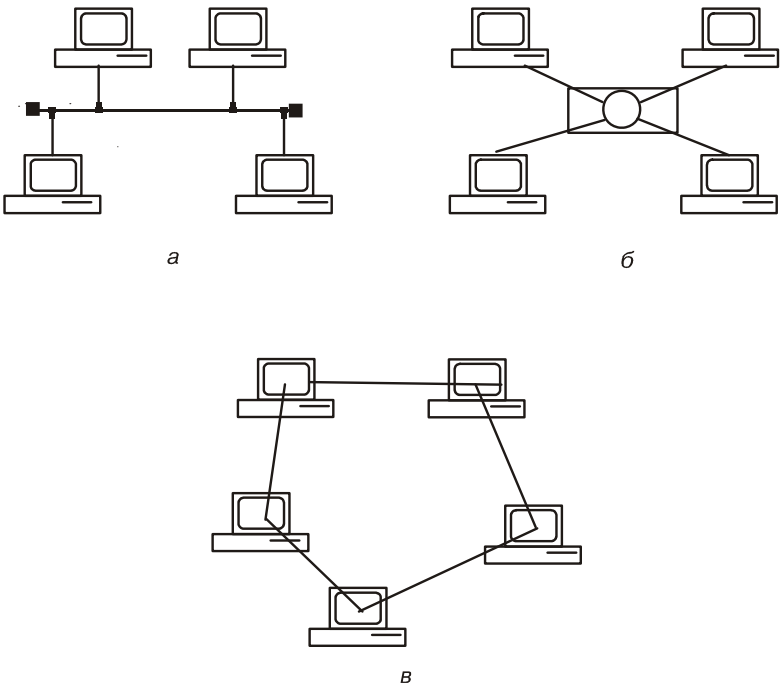


Рис. 2.3. Физические топологии сетей: *а* — шина, *б* — звезда, *в* — кольцо

Стандарты IEEE 802.x определяют технологии, касающиеся двух нижних уровней модели OSI. Состав стандартов 802.x приведен в табл. 2.2.

Таблица 2.2. *Основные стандарты 802.x*

Номер	Наименование
802.1	Internetworking, объединение сетей
802.2	Local Link Control — управление логической передачей данных
802.3	Сети Ethernet
802.4	Сети Token Bus LAN
802.5	Сети Token Ring LAN
802.6	Metropolitan Area Network — сети крупных городов
802.7	Board Technical Advisor Group — группа консультаций по широкополосной передаче
802.8	Fiber Optic Techical Advisory Group — группа консультаций по оптоволоконным сетям
802.9	Integrated Voice and data Networks — интегрированные сети передачи данных и голоса
802.10	Network Security — сетевая безопасность
802.11	Wereless LAN — беспроводные сети

С практической точки зрения наибольший интерес для нас представляют сети Ethernet (802.3) и Fast Ethernet (802.3u). На сегодняшний день это самый распространенный стандарт построения локальных сетей. Причем практически все вновь создаваемые сети строятся по технологии Fast Ethernet. Технология Fast Ethernet отличается от технологии Ethernet только на физическом уровне. Кроме того, в некоторых организациях сети Ethernet еще действуют, поэтому вначале мы рассмотрим технологию Ethernet.

2.3. Технология Ethernet

В зависимости от типа физической среды различают следующие виды стандартов сетей Ethernet:

- 10Base-5;
- 10Base-2;
- 10Base-T;
- 10Base-F.

Однако несмотря на различия в типе физической среды все модификации сетей Ethernet, а также сети Fast Ethernet используют единый метод передачи данных — CSMA/CD (Carrier sense multi access / Collision detection — Метод коллективного доступа с опознаванием несущей и обнаружением коллизий).

Суть этого метода состоит в следующем. Для того чтобы получить доступ к единой разделяемой среде, станция должна убедиться, что среда свободна. Для этого станция постоянно прослушивает среду. Признаком свободной среды является отсутствие несущей частоты.

Если среда свободна, то станция может начать передачу. Все остальные станции обнаруживают факт передачи и прослушивают среду на предмет поиска данных для себя. Та станция, адрес которой совпадает с адресом в передаваемом кадре, распознает, что данные предназначаются ей, принимает их, продвигая данные по стеку протоколов вверх.

Если какой-то узел в этот момент хотел начать передачу, но обнаружил, что среда занята, он будет ожидать, пока среда не освободится.

После окончания передачи все узлы выдерживают паузу, она нужна для предотвращения монопольного захвата сетевой среды.

Поскольку сигнал распространяется в общей среде с конечной скоростью, то узлы фиксируют окончание и начало передачи не одновременно. И если две или более станций начнут свою передачу одновременно или почти одновременно (то есть узел начинает передачу в тот момент, когда до него еще не дошли сигналы от другого узла), происходит неизбежное искажение информации. Такая ситуация называется *коллизией* (collision).

Для распознавания коллизии все станции во время передачи сравнивают передаваемые ими данные и данные в общей среде. Различие этих данных является признаком возникновения коллизии.

При обнаружении коллизии все станции прекращают свою передачу, выжидают случайный интервал времени и при условии, что среда свободна, возобновляют свою передачу.

Для надежного распознавания коллизии необходимо, чтобы время передачи кадра минимальной длины было больше времени двойного оборота (Path Delay Value — PDV), так как в худшем случае сигнал должен пройти дважды между наиболее удаленными друг от друга узлами. Посмотрим на рис. 2.4. В момент времени T станция 1 (она расположена на левом конце сети) начинает передачу. Сигнал начинает распространяться по общей среде и в момент времени $T + t$ достигнет правого конца сети. За незначительный момент времени до того, как сигнал дошел до станции 2, она начинает свою передачу, так как для нее общая среда все еще свободна, ведь сигнал от станции 1 до нее еще не дошел. В момент времени $T + t$ эти сигналы столкнутся, и возникнет коллизия. Сигнал коллизии начнет распространяться по сети от станции 2 к станции 1, и ему снова потребуется пройти

всю дистанцию, теперь уже в противоположном направлении. Таким образом, станция 1 получит сигнал коллизии только в момент времени

$T + t + t = T + 2t$.

Вот почему длина кадра должна быть больше времени двойного оборота.

С понятием коллизии также связано понятие домена коллизий (collision domain) — это часть сети, все узлы которой распознают коллизию, независимо от того, в какой части сети коллизия произошла. Домен коллизий представляет собой единую разделяемую среду. Концентратор образует единый домен коллизий. Коммутаторы и маршрутизаторы делят сеть на несколько доменов коллизий (рис. 2.4).

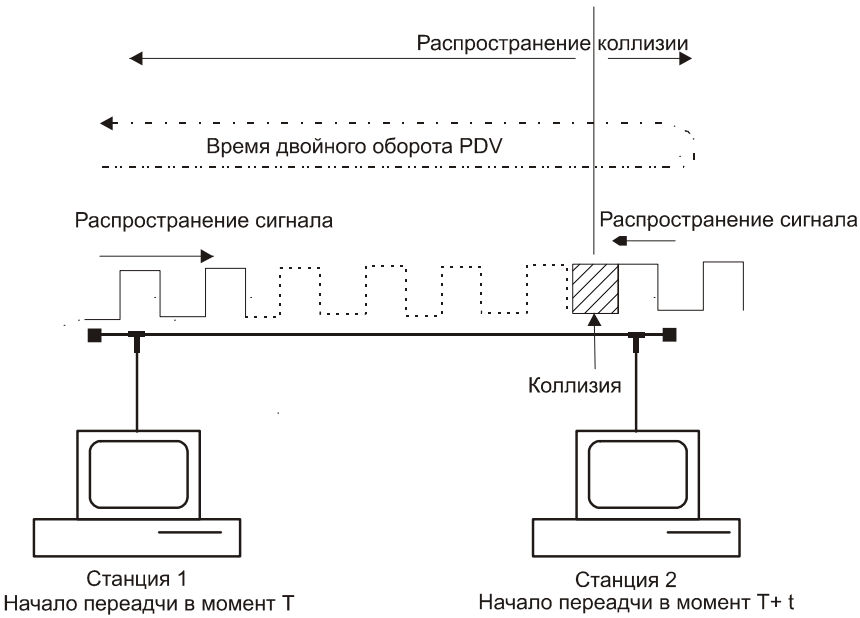


Рис. 2.4. Распространение коллизии и время двойного оборота

Стандарты 10Base — это не что иное, как спецификация физической среды передачи. Рассмотрим подробнее эти стандарты.

- 10Base-5 представляет собой коаксиальный кабель диаметром 0,5 дюйма с волновым сопротивлением 50 Ом. Максимальная длина сегмента сети без повторителя до 500 м. Подключение компьютера к кабелю осуществляется при помощи специального устройства — *трансивера* (transiver). Расстояние между трансиверами не менее 2,5 м. Поэтому для удобства на кабеле, как правило, наносятся метки. На концах сети обязательно должны стоять согласующие терминаторы, препятствующие отражению сигнала от концов кабеля. В противном случае в кабельной системе

возникают *стоячие волны*, и некоторые узлы получают сигнал слишком низкого уровня. В результате сеть оказывается неработоспособной. Стандартом допускается не более 4-х повторителей в сети и не более 3-х нагруженных сегментов.

- 10Base-2 представляет собой коаксиальный кабель диаметром 0,25 дюйма с волновым сопротивлением 50 Ом. Станции подключаются к кабелю при помощи специального Т-образного коннектора. Расстояние между станциями не менее 1 м. Поэтому для удобства есть разметка. На концах кабеля также устанавливаются терминаторы. Стандартом допускается не более 4-х повторителей в сети и не более 3-х нагруженных сегментов. Максимальная длина сегмента сети без повторителя до 185 м. Стандарт 10Base-2 очень напоминает 10Base-5.
- 10Base-T представляет собой UTP-кабель (Unshielded Twisted Pair — неэкранированная витая пара). Используется кабель третьей категории. В данном случае категория определяет полосу пропускания кабеля и некоторые другие характеристики. Используется две пары кабеля: одна для передачи от станции к повторителю, вторая для передачи от повторителя к станции. Максимальная длина сегмента сети без повторителя до 100 м. Максимальная скорость передачи данных 10 Мбит/с. Сети на основе UTP-кабеля строятся по звездообразной топологии. В центре звезды находится *концентратор* (hub). Концентратор повторяет сигнал, пришедший на его вход, на все его выходы. Таким образом, реализуется единая разделяемая среда. В случае возникновения коллизия передается на все входы путем посылки специальной jam-последовательности. При соединении концентраторов друг с другом их число между любыми двумя станциями не должно превышать 4-х (правило четырех хабов). При необходимости соединения нескольких хабов логически целесообразно организовать древовидную структуру и использовать более жесткое правило 3-х хабов.
- 10Base-F — физическая среда построена на основе волоконно-оптического кабеля. Оптическое волокно может быть многомодовое с полосой пропускания 800 МГц или многомодовое с полосой пропускания 2—3 ГГц. Оптический кабель на основе многомодового волокна более дешевый и более простой в монтаже. Построение сети аналогично построению сети 10Base-T. Имеет два стандарта спецификации: 10Base-FL, 10Base-FB. Отличаются стандарты мощностью передатчиков, а как следствие, и максимальным расстоянием между элементами сети (до нескольких километров). Сети строятся по звездообразной топологии, в случае соединения нескольких концентраторов топология должна быть древовидной.

При расчете сетей, построенных по технологии Ethernet, важно соблюдать множество ограничений для сетей этого класса (рис. 2.5). Основными

правилами является правило 4-х хабов (как правило, оно вырождается в правило 3-х хабов) и ограничение длины одного сегмента (табл. 2.3). Есть еще условия, которые при построении небольшой сети вам вряд ли придется соблюдать: это ограничение максимального количества узлов (< 1024), а также соблюдение ограничения для времени двойного оборота. Последние ограничения сказываются только в очень больших сетях или сетях, построенных на основе нескольких подсетей различного физического уровня. Методики расчета мы приведем, когда будем рассматривать сети Fast Ethernet. Мы приведем упрощенные методики, если вы захотите более глубоко разобраться в методике расчета сетей, то обращайтесь к соответствующим источникам.

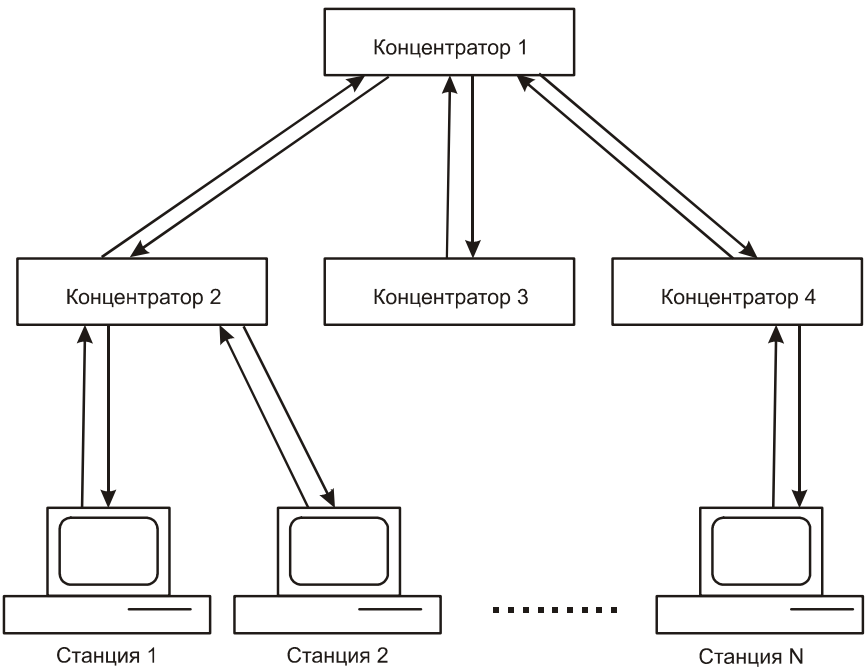


Рис. 2.5. Соединение нескольких хабов в сетях 10Base-T

Таблица 2.3. *Сводная характеристика сетей Ethernet*

	10Base-5	**10Base-2**	**10Base-T**	**10Base-F**
Тип кабеля	Толстый коаксиальный кабель RG-8/11	Тонкий коаксиальный кабель RG-58/U или RG-58A/U	UTP3, UTP4, UTP5	MMF, SMF

Таблица 2.3 *(окончание)*

	10Base-5	10Base-2	10Base-T	10Base-F
Топология	шина	шина	звезда	звезда
Максимальное число узлов на сегменте	100	30	1024	1024
Максимальное количество сегментов	5	5	5 (последоват.)	–
Максимальная длина сегмента	500 м	185 м	100 м	SMF 5 км MMF 1 км
Максимальная длина сети	2500 м (300 узлов)	925 м	500 м	–
Минимальное расстояние между точками включения	2.5 м	0.5 м	–	–
Характер подключения	трансивер	BNC-T-коннектор	RJ-45	SN-коннектор

2.4. Технология Fast Ethernet

С развитием информационных технологий пропускной способности сети, обеспечиваемой технологией Ethernet, стало не хватать. Сеть стала не успевать передавать данные для компьютеров, скорость работы которых существенно возросла. Сетевая среда стала узким местом, отрицательно сказываясь на производительности системы в целом. В результате научных разработок был создан стандарт Fast Ethernet, расширение Ethernet с пропускной способностью до 100 Мбит/с. Этот стандарт получил название 802.3u. Стандарт Fast Ethernet содержит три типа физической среды: 100Base-TX, 100Base-T4, 100Base-FX. Рассмотрим их подробнее.

- 100Base-TX использует 2 пары кабеля UTP или STP (Shielded Twisted Pair — экранированная витая пара). Максимальная длина сегмента сети 100 м. Стандарт рассчитан на применение сетевой топологии типа звезда. Центром сети является концентратор. Соединение кабеля с портом концентратора или сетевой картой осуществляется при помощи разъема RJ-45.
- 100Base-T4 использует 4 пары кабеля UTP третьей категории. По трем парам идет обмен данными, одна задействована для распознавания коллизий. Максимальная длина сегмента сети 100 м. Этот стандарт был